

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
INFORMATION ASSOCIATED WITH FACEBOOK
ACCOUNT WITH USER ID 100008562011804 IN
POSSESSION OF FACEBOOK, INC.

Case No.

19MJ221-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
Title 18 U.S.C. § 1030

Offense Description
Fraud and related activity in connection with computers - unauthorized access

The application is based on these facts:
See affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

7/3/19

City and state:

Durham, N.C.

John Maser
Applicant's signature

JOHN MASER, SPECIAL AGENT, FBI

Printed name and title

Joe L. Webster
Judge's signature

HON. JOE L. WEBSTER, U.S. MAGISTRATE JUDGE

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE
SEARCH OF INFORMATION
ASSOCIATED WITH FACEBOOK
USER ID 100008562011804 THAT
IS STORED AT PREMISES
CONTROLLED BY FACEBOOK
INC.

Case No. 19MTJ221-1

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, John Maser, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since March 21, 2004. I am currently assigned to the Cyber Squad in the Raleigh Resident Agency of the Charlotte Division. I have had this assignment since November 2014. Prior to this assignment, I was a Supervisory Special Agent assigned to the National Cyber Investigative Joint Task Force in Chantilly, Virginia. I have also been assigned to the Philadelphia Division where I investigated public corruption and the Cincinnati Division where I investigated white collar crime matters. Prior to becoming a Special Agent, I was employed as a CPA with an international accounting firm. I have previously conducted Federal criminal investigations involving the use of subpoenas, search warrants, and computer forensic examinations. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030 (computer fraud), 1343 (wire fraud), and 371 (conspiracy) have been committed by various individuals, including those using the Target Facebook Account. There is also probable cause to search the

information described in Attachment A for evidence of these as described in Attachment B.

PROBABLE CAUSE

4. The Federal Bureau of Investigation is investigating a family of malicious software ("malware") known as Emotet, which was first observed in 2014, targeting the banking industry. The malware worked by injecting computer code into an infected computer and stealing sensitive information, including financial and address book data. Since then, it has evolved into a "dropper," which is malware that surreptitiously injects other malware into a computer. Emotet was first discovered in North Carolina, following the infection of a school district's computer network in December 2017. Since that time, there have been numerous other victims throughout North Carolina and the United States, to include computer networks of local, state, tribal and federal governmental units, corporations, and networks related to critical infrastructure.

5. Administrators of the Emotet malware communicate with infected computers through two separate systems of servers, each with a tiered hierarchy, described here as Tier 1, Tier 2, and Tier 3. One system of servers distributes the malware payloads, and the other serves as command-and-control for the malware. When a victim receives a malicious email containing a link to download an infected document, the victim's machine contacts a Tier 1

distribution server. Such servers, which appear to host websites that have been compromised, deliver infected documents and files to the intended victim. There are many Tier 1 servers that communicate with infected computers. These Tier 1 distribution servers receive their malicious files from Tier 2 servers, which pass files and instructions from Tier 3 servers. The Tier 2 servers appear to be compromised and repurposed to send files and instructions from one or more Tier 3 servers.

6. Emotet's tiered infrastructure appears to serve the following purposes: (a) widely disperse the malware distribution to minimize disruption when Tier 1 servers are blacklisted by anti-virus, security, and hosting companies, and (b) obfuscate the actors behind Emotet by creating layers of infrastructure. The lower-tiered infrastructure is comprised of compromised servers operated by legitimate businesses and individuals, while the higher-level infrastructure operated by the Emotet actors may be hosted on bulletproof hosting companies that are not law enforcement friendly.

7. Through analysis of Emotet malware samples and network traffic from computers infected with Emotet, investigators have identified two command-and-control Tier 2 servers and a distribution Tier 3 server. The Tier 3 server, which is sending large amounts of data to Tier 2 distribution servers approximately every 10 minutes, is believed to be controlled by the parties responsible for the Emotet malware.

[REDACTED]

10. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11. [REDACTED]

[REDACTED] is

associated with Nikolai Nikolaevich Egupov, date of birth of 3/18/1984, in St. Petersburg, Russia. Open source queries identified an individual on Russian social media site VK.com matching the name, date of birth, and location of St. Petersburg, Russia. Additional queries determined the profile picture for Egupov on VK.com was identical to that of a Nikolay Egupov on Facebook (<https://www.facebook.com/profile.php?id=100008562011804>). The FBI was able to link Egupov to Facebook account with user ID 100008562011804 — the SUBJECT ACCOUNT.

12. On or about May 7, 2019, investigators obtained subscriber information from Facebook pertaining to the SUBJECT ACCOUNT. The

subscriber results revealed that the email address keshka888@mail.ru and phone number +79216458686 are associated with the Facebook account. The name on the account was "Николай Егупов" which translates to "Nikolai Egupov." The results also revealed that the account is still actively used, and was logged into as recently as April 10, 2019 from IP address 188.243.55.183. IP address 188.243.55.183 was used to log into the account 24 times since the account was created in December 2014. IP address 188.243.55.183 resolves to St. Petersburg, Russia.

13. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

14. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact email addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

15. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

16. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

17. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post

"status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

18. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

19. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user.

Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

20. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

21. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

22. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

23. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been

tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

24. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

25. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

26. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

27. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and

the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

28. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed

or used. For example, as described herein, Facebook logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

30. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

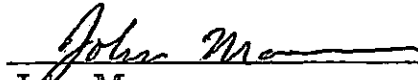
CONCLUSION

31. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

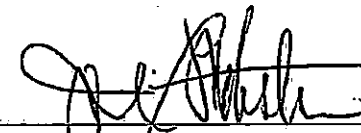
32. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,


John Maser
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on July 5, 2019 9:07 AM


The Hon. Joe L. Webster
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook user ID 100008562011804 that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a social networking company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the ID listed in Attachment A:

1. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact email addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
2. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
3. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

4. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

5. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

6. All other records and contents of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

7. All "check ins" and other location information;

8. All IP logs, including all records of the IP addresses that logged into the account;

9. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

10. All information about the Facebook pages that the account is or was a "fan" of;

11. All past and present lists of friends created by the account;

12. All records of Facebook searches performed by the account;

13. All information about the user's access and use of Facebook Marketplace;

14. The types of service utilized by the user;

15. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

16. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

17. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken; and

18. All records and information relating to machine cookies.

Facebook is hereby ordered to disclose the above information to the government within fourteen (14) days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer fraud), 1343 (wire fraud), and 371 (conspiracy) involving Nikolai Egupov since December 10, 2014, including, for each user ID identified on Attachment A, information pertaining to the following matters:

1. Evidence relating to the Emotet malware or other types of malware or computer fraud schemes.
2. Evidence of relations or communications between Egupov and other conspirators;
3. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
4. Evidence indicating the Facebook account-owner's state of mind as it relates to the crime under investigation; and
5. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this

warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.